SPECIFICATION AMENDMENTS

Please amend the paragraph beginning on page 1, line 28 as follows:

Many copy protection techniques known in the art are limited to computer programs, relying on physical objects which are difficult to copy (such as dongles or media with irregular formatting). The protected program contains special software that tests if the physical object is present and prevents the program from operating if the test fails. This renders copies unusable, since a copy will not function without the presence of the physical object. An example of a technique to fingerprint magnetic media is ~~thought~~ taught in U.S. patent 5,428,683. In such a system, digital information about the individual magnetic disk is stored in the physical object. Copies of the content will be on different physical disks, and the individual information will not match. ~~however~~ However, the physical object must store information about every magnetic media to be protected. The publisher of a new media must therefore create a new physical object with the new information. This is expensive for the end user and requires considerable technical knowledge to install and use the physical objects.

Please amend the paragraph beginning on page 3, line 26 as follows:

Encryption-based systems of this general type are nevertheless used widely for applications including encrypted satellite television broadcasts and encrypted CD-ROMs. In U.S. patent 5,513,260, assigned to MacroVision, Ryan discloses such a copy-protection system. The system uses a combination of symmetric (secret-key) and asymmetric (public-key) data encryption to permit the player to handle either copy-protected or non-copy-protected media. (Both of these types of encryption are well known in the art of cryptography.) An authenticating digital signature is recorded on the media, and the media reader prevents the signature from being transferred to illicit copies. The absence of this signature on copy-protected disks causes the player to generate false data which prohibits the disk from playing normally. Therefore, while this system does nothing to prevent copying, the media reader attempts to regulate the use of copies by searching for the digital signature. While the digital signature mechanism can regulate issuance of new content, the system obviously cannot prevent exact copies of the content media from being produced and used by a reader that does not recognize the digital signature. As with the approach in ~~is~~ U.S. patent 5,034,980, compromise of a player's decryption keys enables attackers to decrypt all content it can play.

Please amend the paragraph beginning on page 6, line 4 as follows:

C13 6. Because software programs will not have access to the decryption keys, software developers will be unable to develop applications to play protected content. Software developers may even be motivated to try to crack the system in order to find the decryption keys required to produce software decoders.

Please amend the paragraph beginning on page 6, line 25 as follows:

C14 There is no perfect solution to the copy protection problem, since attackers with unlimited resources can always find ways to obtain or recreate the content and distribute it. However, it is possible to significantly increase the cost per successful attack. A successful system attempts to satisfy as many of the following constraints as possible:

Please amend the paragraph beginning on page 8, line 26 as follows:

C15 Another object of the invention is to support "copy-once" data which may be recorded once by consumers, but cannot later be recopied. Additionally, it is an object to allow the use of more sophisticated protection mechanisms in conjunction with this invention, including "copy-once" data and to control activation of other protection techniques.

Please amend the four paragraphs beginning on page 10, line 7 as follows:

C96

The present invention provides a method and system for providers of copyrighted content in the form of digital data to mark the data during the manufacturing process, such that consumers of the content can read the data but cannot transfer it to an output device, such as a digital storage or computer network interface, without specific authorization from the copyright owner. Thus, the invention provides a highly effective copy-prevention process that allows manufacturers and publishers to sell or rent copyrighted works with added confidence that sales or rental revenue will not be lost to illegal copying.

In one embodiment of the invention, copyrighted data is produced and stored on physical media for distribution to end users using conventional distribution channels. The publisher creates the digital data representing the original content and transmits it to a computer or processor which marks it ~~using a secret copyright mark, referred to herein as an authenticator, which is computed by applying a masking function to the data~~ using a constant copyright mask, and also a constant override mask derived from a secret value referred to herein as an authenticator. The data and authenticator are then sent to a media writer which mass produces copies of the work ~~(including the authenticator)~~ or produces a master for use in mass duplication of copies. These copies are distributed to end users by conventional means.

The user places the copy in a reader device which reads the data and transmits it to an output device for visual or aural communication to the user by display, playback, printing or the like, depending on the type of data involved. The output device can be a digital storage medium such as a digital versatile disk or alternatively it can be an interface to a computer network. The copyright mark is not visible or audible to the user in the output; however, if the copyright-marked data is sent to a media writer device having a built-in security processor chip, the processor will detect the presence of the copyright mark ~~by recomputing it from~~ in the data and will refuse to write the data to the output device without also detecting a write-permission mark which is also embedded in the data, or receiving a valid authenticator which corresponds to the data.

~~The masking function which is used by the publisher to compute the authenticator or copyright mark, and by the security processor in the user's writer device, to detect the mark is preferably a non-collision resistant compression function, and more preferably the Hamming majority value of a block of data. Data which does not contain an embedded copyright mark can be written normally.~~

Please amend the paragraph beginning on page 14, line 17 as follows:

Referring to FIG 2, the process steps for enforcing copy-prevention in the writer 130 are now detailed. Before content is

written, the writer 130 must determine whether the material is copyright-marked and, if so, whether the write ~~is~~ request is authorized. To accomplish this, the writer must test for copyright identification marks in the data to be written. To perform this test, the data must be divided (either by the processor or elsewhere) into blocks of at least one bit each. In this preferred embodiment, blocks are adjacent, do not overlap, and are of uniform size. However, the system can also use blocks which partially or completely overlap each other, which are not adjacent, or which are not of uniform size. The block division algorithm may exclude any unused data (such as comments) to prevent attackers from trying to disable protection marks by inserting or modifying unused data regions. For each block to be written, the copy-protect mechanism inside the writer undertakes the following steps:

Please amend the paragraph beginning on page 15, line 26 as follows:

(5) Check (270) shift register for copyright indicator. In the preferred embodiment, this checking process is implemented by testing whether at least 62 of the least significant 64 bits of the shift register match the global copyright mask, a pre-defined 64-bit system-wide constant value. If there is no match, the write request is allowed to proceed (290). If the global copyright mask is detected, the data is assumed to be copyright marked. Note that the probability of an erroneous match is

C18

vanishingly small; the probability of an accidental match in 62 of 64 bits is about 1 in ~~1016~~ 10^{16}.

Please amend the paragraph beginning on page 17, line 22 as follows:

C19

The FIG 2 approach can also be used to restrict content playback. For example, a publisher might wish to restrict playback by player type, player manufacturer, geographical region, player authorization, etc. Each player is preprogrammed with a set of global copyright masks and/or content override masks corresponding to content it will refuse to play. Players can also contain a set of masks corresponding to content they are expressly authorized to play. At step 270, the shift register is checked against each of these masks. If a content-forbidden mask is found or if content-acceptable masks are required but not present, the player refuses to play the content.

Please amend the paragraph beginning on page 19, line 4 as follows:

C10

A specific WCEP implementation will now be described which includes six shift registers loaded using different block lengths. FIG 4 ~~is~~ lists the writer state variables (400) for the specific implementation to be described. In this embodiment, the writer needs approximately 993 bits of state information. No nonvolatile storage is required; all state information may be stored in RAM. On power-up, insertion of a new media disc, etc.

all register contents should be reset to zero. S0 (401), ~~S1,~~ S1 (402), S2 (403), S3 (404), S4 (405), and S5 (406) are each 128-bit shift registers. C1 (407), C2 (408), C3 (409), C4 (410), and C5 (411) can each be 16-bit counters, though some can be made smaller. A1 (412), A2 (413), A3 (414), A4 (415), and A5 (416) are also each 16-bit or smaller counters. B (417) is a 1-bit register. Finally, X (418) is a 64-bit field used as the content override mask.

Please amend the four paragraphs beginning on page 21, line 24 as follows:

Test if A1 equals 5 (608). If so, set S1 equal to S1 shifted left one bit. If C1 is less ~~then~~ than three then make the least significant bit of S1 equal to zero, otherwise make this bit a one (609). Next, perform CopyrightCheck on S1 with the global copyright mask 0xC84D57481F7D5757 (610). Finally, set both A1 and C1 to zero (611).

Test if A2 equals 31 (612). If so, set S2 equal to S2 shifted left one bit. If C2 is less ~~then~~ than 16 then make the least significant bit of S2 equal to zero, otherwise make this bit a one (613). Next, perform CopyrightCheck on S2 with the global copyright mask 0x92ABC79E99F157FC (614). Finally, set both A2 and C2 to zero (615).

Test if A3 equals 128 (616). If so, set S3 equal to S3 shifted left one bit. If C3 is less ~~then~~ than 64 then make the

least significant bit of S3 equal to zero, otherwise make this bit a one (618). Next, perform CopyrightCheck on S3 with the global copyright mask 0xC84D57481F7D5757 (618). Finally, set both A3 and C3 to zero (619).

C11

Test if A4 equals 1024 (620). If so, set S4 equal to S4 shifted left one bit. If C4 is less ~~then~~ than 512, then make the least significant bit of S4 equal to zero, otherwise make this bit a one (621). Next, perform CopyrightCheck on S4 with the global copyright mask 0x92ABC79E99F157FC (622). Finally, set both A4 and A5 to zero (623).

Please amend the paragraph beginning on page 26, line 13 as follows:

C12

The reader will appreciate that this protection system can be combined with traditional encryption-based copy protection systems to provide the security advantages of both. Content can be embedded with copyright marks after it is encrypted, thereby preventing would-be attackers from copying the ciphertext. Content can also be marked before it is encrypted to provide copy resistance even if attackers recover the encryption keys from a player.

Please amend the paragraph beginning on page 27, line 17 as follows:

C13

Other preferred embodiments of the invention will be apparent to those skilled in the art from a consideration of this

specification or practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with the true scope and spirit of the invention being indicated by the following claims. ~~GLOSSARY Authenticator: The authenticator (denoted with the variable Y) is a secret value generated by the publisher which enables a copyright marked piece of content to be written. Consumer: A purchaser of some protected content who may want to make unauthorized copies of it. Content: Data which a publisher wishes to protect against unauthorized copying. Content Marking System (CMS): A system used by the publisher to embed the global copyright mask and content override mask in content. Content Override Mask: The content override mask (denoted with the variable X) is computed from the authenticator using a secure hash function. The content override mask is (along with the global copyright mask) embedded in the data by the CMS. A writer only allows copyright marked content to be written if it has been supplied with an authenticator which hashes to the content override mask. Global Copyright Mask: A global constant used to identify copyright marked content. Publisher: The owner of some content which is to be protected. Reader: A device which reads content from a digital storage medium. In other embodiments, the reader can be a network interface, digital radio receiver, etc. Writer: A device which writes content to a digital storage medium, such as a DVD, hard disk, etc. In other embodiments, the writer can be a network interface, broadcast mechanism, etc.~~

~~Consumers and publishers both own writers, which can have identical capabilities. Writer Copy Enhancement Processor (WCEP): A processor in each writer which rejects attempts to write copyright marked data unless a proper authenticator has been provided.~~

Please amend the paragraph beginning on page 28, line 23 as follows:

Content Override Mask: The content override mask (denoted with the variable X) is computed from the authenticator using a secure hash function. The content override mask is (along with the global copyright mask) embedded in the data by the CMS. A writer ~~only~~ allows copyright-marked content to be written only if it has been supplied with an authenticator which hashes to the content override mask.